Mend.io general compliance & accreditations overview

As a provider of secure development tools, Mend.io's first priority is to maintain a safe and secure environment for its customers.

To ensure the highest level of security, we constantly invest in our overall information security program, resources and expertise.

Here at Mend.io, we understand the importance in providing clear information about our security practices, tools, resources and responsibilities, so that our customers can feel confident in choosing us as a trusted service provider and understand how and what we do in order to secure our platform.
For additional assurance we undergo regular independent verification of our information security and compliance controls to ensure we can consistently demonstrate continued compliance and provide the assurance you need to feel secure when using our products.

Mend.io is proud to be externally verified as compliant to the following standards and can provide supporting evidence and information about the controls we have in place in relation to these standards.
We also have several resource documents and mappings for compliance support when formal certifications or attestations may not be required or applied.

- ISO 27001:2013 Information Security Management

An internationally recognized standard, governing the protection of information assets. This ISO standard certifies that our management system conforms to rigorous security standards, in particular for managing security risks.

At Mend.io, we have fully implemented the ISO 27001:2013 standard. Our Statement of Applicability (SoA) allows our customers to review our set of controls and see which policies we have in place to meet the control requirements. Customers can then use this information to determine which controls apply to them and how these controls are managed within our organization.

- AICPA SOC2 SSAE 18 /ISAE 3402 Type II

The SOC2 is a report based on the auditing Standards Board of the American Institute of certified Public Accountants (AICPA) existing Trust Services Criteria (TSC)
This report provides an external evaluation of an organization's internal security systems with a specific focus on the controls relevant to security, availability and confidentiality. A copy of this report can be requested via the customer's account team.

- Other accreditations not mentioned above.

Mend.io is dedicated to continual improvement and the frameworks we are compliant with ensure this is a key focus for the organization. The frameworks we have implemented are industry recognized standards that are fully applicable to the type of services we provide.

- Laws / regulations

Mend.io takes data protection very seriously. As a global company with operations in the USA, Israel and Europe, Mend.io is fully committed to compliance with the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) as well as any other laws it is subject to.

Whilst there is no formal certification of our compliance we can offer our customers, adherence to all relevant information security regulations and legislation is externally validated as part of our ISO and SOC2 program as well as by our team of dedicated internal auditors on a regular basis.

Furthermore, Mend.io is committed to providing visibility of all privacy related policies and associated agreements. Our privacy policy gives you information on how we handle personal data, the way we use it and your rights in respect of your data.

To enhance data protection, we have implemented technical and organizational measures to minimize personal data processing and ensure that only necessary data is processed. In particular, we pseudonymize the email addresses of our customers' contributing developers using encrypted email addresses through hashes.

Additionally, we have partnered with TrustArc as our Dispute Resolution Service Provider for unresolved privacy concerns data subjects' may have, adding an extra layer of trust and transparency. It satisfies the Independent Recourse Mechanism requirement for the EU-US Data Privacy Framework, which includes coverage for both Swiss-US and UK Extension.

- Insurance

Mend.io maintains adequate insurance policies against Cyber attacks. At the point of time this document was created Mend.io maintains the following insurance policies:

- Professional Indemnity
- Cyber
- Director and Officers Liability
- Corporate Legal Liability
- Employment Practices Liability
- Public Liability